Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 335-358

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

IRELAND

1. Legal Sources

In the Republic of Ireland, this area is generally unregulated by law.

The Irish parliament has passed **no legislation specific to internet content**[1] and of the **Council of Europe Conventions** related to illegal internet content, the Republic of Ireland has **ratified only the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. The requirements of that treaty have been transposed into Irish domestic law by the Data Protection Act 1988, as amended.

The **blocking and take-down of internet content** which breaches provisions of Irish criminal law can at present be achieved **only under two soft law mechanisms** created by commercial operators of internet access and/or hosting services.[2] Both are restricted to online activity constituting a very **limited range of criminal offences**. Three mobile telecommunications operators in Ireland block access by Irish subscribers to a list of IP addresses at which child sexual abuse content has been found. All the members of the Internet Service Providers Association of Ireland remove from the internet any material which is hosted by them, is reported to the Irish Internet Hotline and is found to constitute one or more criminal offences associated with child sexual abuse (child pornography, child trafficking, child sex tourism or the grooming of children for sex), incitement to hatred on racial, xenophobic or other grounds, or financial fraud.

The principles of common law and equity applied by the Irish courts have developed mechanisms which permit victims of torts (breaches of legal norms entailing civil responsibility) to obtain judicial orders in **civil proceedings for the removal of the internet content constituting or contributing to the tort**.[3] These mechanisms were originally developed in response to claims of breaches of intellectual property rights, in particular online breaches of copyright. The principal remedy of a mandatory injunction, requiring removal of infringing material from the internet, could be granted in this context only after the European Union (Copyright and Related Rights) Regulations 2012 amended the Copyright and Related Rights Act 2000 so as to properly transpose the European Union's Information Society Directive. At least as a matter of legal principle however, the mechanisms are equally available to victims of other torts, in particular defamation and breaches of data protection principles causing loss to the data subject.

---

1 Refer to the officially published *Report of the Internet Content Governance Advisory Group*, Dublin: Department of Communications, Energy and Natural Resources, 2014, p. 50, after Fn. 164.

2 Refer below, to point 2.2.2. of the present national report.

3 Refer below, to point 2.2.1. of the present national report.

2. Legal Framework

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. Legal mechanisms for blocking

There is at present **no basis[4] in Irish law for blocking and/or filtering** internet content, even if its dissemination constitutes a criminal offence or it is otherwise unlawful in Ireland.

At the **level of practice**, the **Irish national police force** (*An Garda Síochána*) has concluded an **agreement with an Irish provider of mobile telephone services**, under which agreement the mobile service provider takes certain steps with respect to certain internet content accessible via later generation mobile phones. The Office of the Commissioner of *An Garda Síochána* has confirmed[5] that the police force has agreed upon a memorandum of understanding with one Irish service provider, under which the provider will block customer access, using the mechanism of so-called "DNS poisoning", to specified sites containing confirmed child pornographic material. The sites are those placed by INTERPOL on its "worst of list" and subsequently furnished by *An Garda Síochána* to the service provider in encrypted form. According to the Office of the Commissioner, the operation of this agreement has been assessed as effective and valuable. Through ongoing engagements with other service providers, the police have received expressions of interest in coming to similar agreements. It is envisaged that blocking access to identified child pornographic material will become an industry standard in Ireland. Progress in this regard is being made and *An Garda Síochána* is committed to even greater progress as a priority. For example, the police force works closely with Hotline.ie and is provided with anonymised internet content relative to suspected child pornography URLs.[6] The police force considers that there is an investigative value in this beneficial relationship. On the other hand, as *An Garda Síochána* has no direct role in blocking access to, filtering out or removing internet content, the organisation has no formal written policy on that specific issue.

---

4 Refer below however, to the fourth paragraph under point 2.2.1.1. in the present national contribution. Pars. 40(5A)(a) and 205(9A)(a) of the Copyright and Related Rights Act 2000 are formulated in extremely general terms; they permit the High Court, on the application of a holder of copy- or related rights, to issue “an injunction against an intermediary”. Such an injunction could require an Irish internet access provider to block users’ access to internet content which (allegedly) breaches the copy- or related rights of the applicant(s) for an injunction (refer to T.J. McIntyre, Everything you need to know about Ireland’s SOPA, published in electronic form on the website of thejournal.ie (http://jrnl.ie/335983) on 24.01.2012 and last consulted on 25.04.2016). According to a media report (http://jrnl.ie/948503 - last consulted on 25.04.2016), Justice McGovern of the Irish High Court did in fact issue such an injunction in 2013, against six Irish internet access providers, ordering them to block access to Pirate Bay. In the time available for its finalisation, the author of the present national contribution has been unable to confirm the accuracy of that report or determine the extent to which the requirements of any injunction were actually carried out.

5 By e-mail of 11 December 2015 received by the author of the present national contribution from Mr. Michael McElgunn, Inspector for Superintendent in the Office of the Commissioner. The Commissioner is the most senior Irish police officer, responsible for the operational management of the entire police force, subject to the directions of the Minister for Justice, Equality and Law Reform (refer to http://www.garda.ie/Controller.aspx?Page=19&Lang=1 - last consulted on 11.12.2015).

6 This mechanism will be described in detail below, under points 2.2.2. and 3.3. of the current national contribution.

2.1.2. Soft law mechanism for blocking

A **soft law mechanism** of very limited scope operates in Ireland to deal specifically with internet content which potentially breaches Irish criminal law in respect of **child sexual abuse**. The mechanism is applied by **four mobile telecommunications operators** in Ireland who are members of the Mobile Alliance Against Child Sexual Abuse Content.[7] This "Alliance" is actually an initiative of some of the members of the European regional grouping of the umbrella association of mobile telephone network operators – GSMA.[8] The Alliance pursues a number of interrelated policies of technical intervention, cooperation and information sharing, aimed at creating significant barriers to online access to child sexual abuse content[9] and in particular the commercial exploitation of such content. It is formally recognised by the European Commission and by the International Telecommunication Union. One of the technical measures is that of blocking access by Irish subscribers (mobile telephone users) to a list of IP addresses which is constantly updated by the Internet Watch Foundation of the United Kingdom.[10]

2.2. Take-down/removal of illegal Internet content

2.2.1. Legal mechanism for removal

2.2.1.1. Online copyright infringements

A removal mechanism is provided by Irish law to owners of **intellectual property rights**.

This mechanism was created by the law of equity, as applied and developed by the Irish courts in cooperation with the courts of other common law jurisdictions. It permits a court to make an order (a so-called "**Norwich Pharmacal order**"[11]) on the application of a victim of tortious conduct against a respondent who is not necessarily a (co)author of the tort, but knows or has the means to easily discover the identity of the tortfeasor(s). The respondent is **required to inform the applicant of the identities of the tortfeasors**, who can then be joined by the applicant as additional defendants to the proceedings and thus made to answer the applicant's claims for damages (financial compensation) and/or injunctive relief (usually in the form of a judicial order that each defendant discontinue or refrain from repeating the tortious conduct in the future).

---

7 An overview of this initiative is available on the GSMA website: http://www.gsma.com/publicpolicy/wp-content/uploads/2013/10/GSMA_The-Mobile-Alliance-Against-Child-Sexual-Abuse-Content_Oct-2013_2ppWEB.pdf (last consulted on 07.07.2015).

8 Technically an acronym for Groupe Spéciale Mobile Association. The *Groupe Spéciale Mobile* was originally formed in the 1980s in order to develop a pan-European standard for mobile telephony and thus permit calls to be made across the mobile networks of more than one country. This resulted in the adoption of a "GSM standard". The various enterprises offering mobile telephone services on that standard therefore formed the "GSM Association".

9 This concept includes child pornography, but also covers child trafficking and other illegal activities directly affecting children.

10 This information was provided to the author of the present national report by Mr. Paul Durrant, Chief Executive of the Internet Service Providers Association of Ireland, during a discussion held on 05.06.2015. Refer also to the description provided by the Irish Office for Internet Safety on its website (http://www.internetsafety.ie/website/ois/oisweb.nsf/page/regulation-mobilephone-en - last consulted on 24.08.2015), under the heading "Mobile action against child sexual abuse content (child pornography)".

11 Named after the British case of *Norwich Pharmacal Co*. *et al*. v. *Customs and Excise Commissioners*, [1974] Law Reports, Appeal Cases 133, House of Lords, in which this type of relief was accorded for the first time.

In the landmark case of *EMI Records (Ireland) Limited et al*. v. *Eircom Limited* and *BT Communications Ireland Limited*,[12] Mr. Justice Kelly of the High Court of Ireland held that the applicant owners of intellectual property rights could obtain a **Norwich Pharmacal order against the respondent internet access providers**, requiring them to inform the applicants of the names and physical addresses of certain of their customers who held specified IP-addresses and were offering "pirated" copies of works in which the applicants held the Irish copyrights. That was a logical application of the equitable principle, as the applicants had convinced the court *prima facie* that they were victims of the statutory tort of copyright infringement and that they could not identify the tortfeasors without the assistance of the respondent internet access providers.

In the result, since the middle of 2005, owners of Irish intellectual property rights have been effectively able to obtain **injunctive relief against online copyright infringers**, effectively obliging them to "take down" or remove the infringing internet content.[13] Applications for injunctions are usually accompanied by potentially highly dissuasive applications for financial compensation, including for the costs of the legal proceedings. The most important holders of Irish copyrights were nevertheless dissatisfied with this mechanism[14] and subsequently tried to obtain injunctive relief directly against internet access providers, requiring the latter to discontinue the provision of access services to online infringers and thus put a stop to their infringing activity by means of the internet. This remedy is now available under subsections 40(5A) and 205(9A) of the Copyright and Related Rights Act 2000. Those provisions effectively empower the High Court of Ireland to grant injunctions against internet "intermediaries" on an equitable basis. Referring to only two considerations, which need to be taken into account only in appropriate circumstances, the legislation effectively gives the High Court an entirely discretionary power:

> "… [T]he court shall have due regard to the rights of any person likely to be affected by virtue of the grant of any such injunction and the court shall give such directions (including, where appropriate, a direction requiring a person be notified of the application) as the court considers appropriate in all of the circumstances".[15]

It should be noted that those provisions were not originally included in the Copyright and Related Rights Act 2000. They were introduced by paragraph 2 of the European Union (Copyright and Related Rights) Regulations 2012. These regulations[16] were made in reaction[17] to a judgment[18] of the High

---

12 [2005] 4 Irish Reports 148.

13 Refer to K.T. O'Sullivan, "Irish Digital Rights in Retrograde: the 'Eircom Protocol' and the Normative Framework of European Law", in (2013) 36 *Dublin University Law Journal* 358, at 371 to 372.

14 In the course of his judgment in the case of *EMI Records (Ireland) Limited et al.* v. *UPC Communications Ireland Limited*, High Court of Ireland, unreported judgment of 11.10.2010, available in electronic format as [2010] IEHC 377 on the internet site of the Irish Legal Information Initiative: http://www.ucc.ie/
law/irlii/index.php (last consulted on 02.07.2015), Mr. Justice Charleton intimated, at par. 62. of his judgment, that it is often practically impossible to recover any compensation from the students and other young people who most frequently carry out the "pirate copying" of protected works.

15 Copyright and Related Rights Act 2000, pars. 40(5A)(b) and 205(9A)(b).

16 Formally designated as Statutory Instrument No. 59 of 2012. The electronic text is freely available on the website for Irish legislation (*electronic Irish Statute Book*) which is operated by the Irish government, but does not have the official status reserved to legislation printed by the Irish government printer: http://www.irishstatutebook.ie/pdf/2012/en.si.2012.0059.pdf (last consulted on 02.07.2015).

17 Refer to B. Hallissay, "Eircom, Injunctions and the European Union (Copyright and Related Rights) Regulations 2012", in 2013 (No. 4) *Irish Law Times* 53. The same conclusion was reached by Mr. Justice Charleton at the end of his judgment in the case of *EMI Records (Ireland) Limited et al.* v. *UPC Communications Ireland Limited*, *op. cit*.

18 In the case of *EMI Records (Ireland) Limited et al.* v. *UPC Communications Ireland Limited*, *idem*.

Court of Ireland that the plaintiff intellectual property rights owners were not entitled to injunctive relief against an internet intermediary, because the subject was entirely regulated by legislation which did not provide for that type of remedy. It has therefore become clear to the Irish judiciary and legal commentators[19] that the Republic of Ireland had previously failed to **transpose the relevant provisions of the European Union's Information Society Directive**[20].

Efforts are currently being made, by the Irish subsidiaries of the major global sound recording enterprises, to take advantage of the new provisions. These **efforts proceed on the basis of an agreement** previously entered into voluntarily[21] by Eircom, the former public monopoly telecommunications service of Ireland and still holder of the largest share of the Irish telecommunications market. That agreement foresees that the recording enterprises will employ surveillance software enabling them to log the IP-addresses of users who up- or download copyrighted material, as well as the title of the material uploaded or downloaded and the date upon and time at which this occurred. This information is passed to Eircom, which identifies the relevant subscribers and notifies them that they have breached their contractual undertaking to Eircom to refrain from using the internet access mechanism in a manner that infringes copyright. The subscribers are warned by Eircom on two occasions that persistent breaches will result in Eircom's termination of the internet access service. If a subscriber is identified on a third occasion, she receives a further warning and her internet access is suspended by Eircom for one week. If she is identified on a fourth occasion, Eircom **permanently ceases to provide her an internet access service**.[22] This arrangement is commonly referred to by critics as a policy of "three strikes, you're out"[23] and by the commercial music recording industry as a "graduated response scheme".[24]

In the case of *Sony Music Entertainment (Ireland) Limited et al.* v. *UPC Communications Ireland Limited* (No. 1),[25] the recording enterprises **applied** under subsection 40(5A) of the Copyright and Related Rights Act 2000 **for the issuance of a mandatory injunction obliging UPC to implement a similar scheme**. Mr Justice Cregan held that he would exercise the discretionary power of the High

---

19 Refer for example to Hallissay, "Eircom, Injunctions and the European Union (Copyright and Related Rights) Regulations 2012", *op. cit*, at Fn. 7 and 8, citing the case of *EMI Records (Ireland) Limited et al.* v. *UPC Communications Ireland Limited*, *idem* and to T. Dillon, "Ireland", freely available on internet at http://graduatedresponse.org/new/?page_id=18 (last consulted on 11.08.2015).

20 Paragraph 3 of Art. 8 of the Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society.

21 I.e. in settlement of litigation commenced by the recording enterprises against Eircom with the aim of obliging Eircom to take action against those of its subscribers who were shown to have repeatedly copyrights belonging to the enterprises; refer to par. 1.1 of the unreported judgment of Mr. Justice Charleton of the High Court of Ireland in the case of *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, available in electronic format as [2012] IEHC 264 on the internet site of the Irish Legal Information Initiative: http://www.ucc.ie/law/irlii/index.php (last consulted on 11.08.2015).

22 This description of the arrangement paraphrases par. 1.1 of the unreported judgment of Mr. Justice Charleton of the High Court of Ireland in the case of *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, *ibid*.

23 Refer to O'Sullivan, "Irish Digital Rights in Retrograde: the 'Eircom Protocol' and the Normative Framework of European Law", *op. cit*, at Fn. 1 and the text of Fn. 2, citing earlier writings.

24 Refer to Dillon, "Ireland", *op. cit*. The page is part of an internet site which is named "graduatedresponse.org" and maintained by an English barrister (http://graduatedresponse.org/new/?page_id=32 last consulted on 11.08.2015) in order to provide comparable information about legal developments in this respect in various countries around the world.

25 Unreported judgment of 27 March 2015 of Mr. Justice Cregan of the Commercial Bench of the High Court of Ireland, available in electronic format as [2015] IEHC 317 on the internet site of the British and Irish Legal Information Institute: http://www.bailii.org/ie/cases/IEHC/ (last consulted on 13.08.2015).

Court to grant an injunction. He would not however, order UPC to proceed in the same manner as Eircom. Instead, citing par. 3(a) of Art. 1 of the EU's Telecommunications Framework Directive,[26] he ordered[27] the parties to settle the details of a scheme which guarantees UPC's subscribers "a prior, fair and impartial procedure" deciding whether or not they have actually infringed copyright. His Honour suggested[28] two possibilities in this respect: the appointment of an adjudicator, independent of both the copyright holders and the internet service providers, who will decide whether a "three strikes" penalty should be imposed on a particular subscriber; or the notification, by UPC to the copyright holders under a Norwich Pharmacal order, of the names and addresses of subscribers alleged to have infringed copyright on a third or fourth occasion, allowing the copyright holders to commence judicial proceedings in respect of the infringements. His Honour announced[29] that he would also judge the terms of the draft injunction on the basis of whether the procedure foreseen would be "effective … and dissuasive", but also "proportionate" and "not … unnecessarily complicated or costly". Finally, he stated[30] that the arrangement would only be fair and equitable and that an injunction can therefore only be issued if the costs of operating it are equitably shared between the copyright holders and the internet service provider. As this was one of the principal points of dispute between the parties, His Honour stipulated[31] that the applicant copyright holders would have to pay 20% of the capital costs incurred by UPC in setting up the necessary technical infrastructure and that its running costs would be capped by limiting to 2'500 the number of infringement notifications that can be sent to subscribers each month. The exact terms of the injunction have since been settled and accepted by Mr. Justice Cregan. He has not issued the injunction however, because UPC has lodged an appeal against the judgment and the settled terms of the injunction are being treated as confidential until the appeal is heard.[32]

These developments are **discussed, in the present national report, under the heading** of "take-down / removal", because they in fact follow on from earlier efforts by the major global recording enterprises to have "pirated" copies of protected works removed from the internet.[33] At the global level, these enterprises promote "graduated response schemes" which frequently involve either the removal of "pirate copies" offered for downloading, or blocking and/or filtering out websites which offer such downloads.[34] Neither of these mechanisms is actually employed in Ireland. Instead, an essentially commercial sanction (disconnection of the internet access enabled by an internet service provider) is or could be imposed upon internet users who take advantage of offers to provide "pirate copies".

---

26 Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.

27 *Ibid*, at par. 267 of his judgment.

28 *Ibid*, at pars. 228 *et seq*. of his judgment.

29 *Inter alia* at par. 201 of his judgment, *ibid*.

30 *Ibid*, at pars. 247 *et seq*. of his judgment.

31 *Ibid*, respectively at par. 259 and par. 263 of his judgment.

32 This information was provided to the Institute by Mr. Gerard Kelly, one of the legal counsel representing UPC in the ongoing litigation, in the course of a telephone conversation on 12 August 2015.

33 Refer above, this point of the present national report. Efforts to block access to internet sites (such as "Pirate Bay"; refer to the cases cited in O'Sullivan, "Irish Digital Rights in Retrograde: the 'Eircom Protocol' and the Normative Framework of European Law", *op. cit*, p. 371, Fn. 72), which allow users to search for and contact other users offering copies of protected works, have been substantially reduced since those sites are able to be "hosted in the cloud" rather than at any physical location; refer to http://piratebay.com.co/ (last consulted on 14.08.2015).

34 Refer to the background information available on the "about"-page of the "graduatedresponse"-website maintained by Mr. Thomas Dillon (http://graduatedresponse.org/new/?page_id=5 last consulted on 11.08.2015).

2.2.1.2. Defamation using internet platforms

Norwich Pharmacal orders and injunctive relief are **remedies** which, as a matter of legal principle, should be **available to victims of all types of torts committed through the internet**. The practically most important of these torts is **defamation**.[35] There is at least one case[36] in which these remedies were actually applied for and granted by a judge of the High Court of Ireland. In 2012, Mr. Justice Peart injunctively required YouTube to remove a video and various written statements by third party users that the plaintiff was the principal person appearing in the video. He simultaneously ordered[37] various defendants (including Facebook, Google and Yahoo) to inform the plaintiff of the identities of the third parties who had made the written statements, which the plaintiff had shown on a *prima facie* basis to be defamatory of him, in that they were erroneous and severely damaged his good name and reputation. Justice Peart noted[38] that he could, if the plaintiff had subsequently shown that the defendants were refusing to comply with the injunction and/or orders, have required the arrest of the defendants and/or the sequestration of their assets for contempt of the High Court. A specific legislative basis for the issuance of an injunction was not necessary in that case; subsection 33(1) of the Defamation Act 2009 provides in general for injunctive relief from defamatory statements and that legislation makes no reference at all to defamation in the online context, although it was enacted relatively long after the dawn of the internet age.

The more general question of the **liability of the operators of social media platforms and other internet host providers for defamatory statements made using their services**, arose in Ireland some years earlier, when two businessmen sued the operator of an online chatroom for libel.[39] The plaintiffs claimed that a number of postings, made in the chatroom by third party individuals, were defamatory and caused them loss in their calling or business and that the operator was liable to compensate them for that loss. It was clear that a person who publishes defamatory statements made by third parties is himself completely liable as a matter of general Irish law for the loss caused. The defendant chatroom operator sought to rely upon the defence provided by the EU E-Commerce Directive[40] specifically for the benefit of internet host providers. This defence had been transposed into Irish law by the European Communities (Directive 2000/31/EC) Regulations 2003.[41] Mr. Justice Clarke of the High Court of Ireland held[42] that the defendant, when providing a chatroom as a supplementary service to its registered betting service clients, was acting as an "intermediary service provider" (to use the terminology of the regulations) and could therefore rely upon the defence

---

35 The possibility of such relief is envisaged, at least impliedly, by the authors of the leading Irish textbook on the law of defamation: N. Cox & E. McCullough, *Defamation Law and Practice*, Dublin: Clarus Press, 2014, p. 52, par. [2-71], at Fn. 148 and p. 571, par. [14-105], Fn. 217. Refer also to the *Report of the Internet Content Governance Advisory Group*, Dublin: Department of Communications, Energy and Natural Resources, 2014, p. 46, particularly at Fn. 149 and 151.

36 *McKeogh* v. *John Doe et al, Independent Newspapers (Ireland) Limited et al. third parties*, unreported judgment of 22.01.2012, available in electronic format as [2012] IEHC 95 on the internet site of the Irish Legal Information Initiative: http://www.ucc.ie/law/irlii/index.php (last consulted on 02.07.2015).

37 These orders and injunctions had been issued on an interlocutory basis, at an *ex parte* hearing of the plaintiff's application for urgent relief; refer to the second paragraph of the judgment of Justice Peart, *ibid*. The published judgment is that handed down by Justice Peart some ten days later, after an *inter partes* hearing of the plaintiff's additional applications against various newspaper publishers.

38 In the third paragraph of his judgment, *ibid*.

39 In the case of *Mulvaney* and *Martin* v. *The Sporting Exchange Limited, trading as Betfair*, [2011] 1 Irish Reports 85.

40 Art. 14 of Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

41 Formally designated as Statutory Instrument No. 68 of 2003. The electronic text is freely available on the website for Irish legislation (*electronic Irish Statute Book*), *op. cit*.

42 [2011] 1 Irish Reports 85, at 100 – 101, pars. [51] and [52].

provided by the Directive if it were able to establish that (a) it originally had no actual knowledge that defamatory statements were being posted and (b) it acted expeditiously to remove those statements once it was made aware of their existence. Whether those conditions were actually fulfilled by the defendant, is a question that could not be answered at a hearing of legal issues and was left to be resolved at a trial of all the evidence. As far as we have been able to determine, the trial never took place.[43]

Although he did not expressly rely upon the fact when coming to his legal conclusion, Justice Clarke did note[44] that the defendant had published "rules of the chat room", which included an agreement by each customer not to post any defamatory item. He made no mention of whether the defendant made any attempt to police compliance with those rules. That issue could be of relevance in determining whether the defendant met the possible supplementary condition to protection of internet host providers from liability, namely that the defendant was "… not aware of facts or circumstances from which [the defamation wa]s apparent".[45] According to a recent report to the Irish government,[46] internet host providers in Ireland presume that **hosts who "moderate" statements made by users** in chat rooms or on other social media platforms are likely to be liable for any damage caused by statements which they do not remove, intentionally or by inadvertence. Under the Irish law of defamation, a person who publicly disseminates a defamatory statement made by another can be liable as a "publisher" of the statement if he disseminated it intentionally, or inadvertently in circumstances in which it was foreseeable that the statement would be disseminated if the person failed to take due care.[47] The few legal sources of relevance in the online context have recently indicated that a platform provider, who actually knows that a particular statement is going to appear on the platform and allows this to happen, will be liable as a publisher, to the same extent as the author.[48] A platform provider, who has no prior indication of the existence of a particular statement intended to be posted by an author, cannot be made liable as a publisher.[49]

---

43 Refer to E. O'Dell, *Mechancial [sic.] turks, safe harbours, and immunities – liability for defamatory comments on websites*, blog posting of 12.10.2010 on http://www.cearta.ie (last consulted on 02.07.2015), stating that the trial had not commenced then (some 18 months after Justice Clarke had handed down his judgment). It is likely that the parties to the litigation reached a settlement, or that the plaintiff's simply withdrew their claim on the basis of a pessimistic assessment of the likelihood of their success at trial.

44 [2011] 1 Irish Reports 85, at 88 – 89, par. [4].

45 Under Art. 18(1)(a) of the European Communities (Directive 2000/31/EC) Regulations 2003, a provider of internet hosting services who wishes to rely upon the defence provided by the Directive must always show that it had no actual knowledge of the relevant unlawful activity, *in situ* the making of defamatory statements. If a claim for damages is being made against the provider, it must also show that it was not aware of any "facts or circumstances" which rendered that activity "apparent".

46 *Report of the Internet Content Governance Advisory Group*, *op. cit*, p. 38, at Fn. 109 and 110.

47 Refer to Cox & McCullough, *Defamation Law and Practice*, *op. cit*, p. 23, par. [2-05], especially at Fn. 11, p. 37, par. [2-35], at Fn. 77 and p. 41, par. [2-46], Fn. 94.

48 *Bunt* v. *Tilley et al*, [2007] 1 Weekly Law Reports 1243, at p. 1249, par [21] of the judgment of Mr. Justice Eady of the Queen's Bench Division of the High Court of Justice of England and Wales. The passage is quoted in P. Milmo & W.V.H. Rogers [eds], *Gatley on Libel and Slander*, 11th ed, London: Sweet & Maxwell / Thomson Reuters, 2008, p. 183, par. 6.18, at Fn. 147 and the case is cited in Cox & McCullough, *Defamation Law and Practice*, *op. cit*, p. 41, par. [2-46], Fn. 94.

49 *Bunt* v. *Tilley et al*, *ibid*, par [23]. The passage is quoted in Milmo & Rogers [eds], *Gatley on Libel and Slander*, *op. cit*, p. 182, par. 6.18, at Fn. 141 and in Cox & McCullough, *Defamation Law and Practice*, *op. cit*, p. 43, par. [2-50], at Fn. 99. The plaintiff's claim in that case was against internet service providers, but in the case of *Metropolitan International Schools Ltd* v. *Designtechnica Corp*, [2009] Entertainment and Media Law Reports 27, Mr. Justice Eady reached the same conclusion in respect of a search engine operator on the basis that the operator had taken no positive step in permitting the appearance of the particular search results.

In between those two extremes, a platform provider who learns of the existence of a statement to be posted, for example because its moderation team sees the statement submitted for posting, will be liable as a publisher if it is foreseeable that the statement would defame a third party.[50] The Irish sources contain no analysis of the meaning of the term "apparent", employed in formulating the legislative defence available to intermediary service providers and it might well be interpreted by an Irish court as akin to "foreseeable" in the sense already known to Irish law.[51] It is also clear from the principles of Irish law described above, that such a provider cannot be liable as a publisher at all, if it has no active involvement in the process of publication on its platform. Providers in Ireland therefore usually undertake no moderation activities at all. Although there probably is a demand for moderated platform services, most of the Irish internet host providers have captured quite small parts of the market and consider that it would not be commercially viable to raise their prices in order to cover the cost of providing (relatively labour intensive) moderation services.[52] The policy of non-moderation limits costs and avoids liability.

2.2.1.3. Online data protection infringements

Another tort which could be committed online is that of **negligence in the treatment of personal data** and a data subject could in principle apply for a Norwich Pharmacal order and injunctive relief as part of a claim against a data controller. A recent report to the Irish government states[53] that internet users who post personal information, including videos or still images, about third persons without their consent, as well as internet host providers who knowingly permit this to happen or (more frequently) fail to remove such material once made aware if its existence, would be liable to the third persons under Irish law. The Data Protection Act 1988, as amended, provides[54] for **tortious liability to persons who suffer loss as a result of a failure to comply with the data protection principles** set out in and within the framework created under that legislation.[55] The report also points out[56] that public awareness of data protection principles and of personal legal rights in that respect is very low in Ireland. Data subjects who are aware of their substantive rights generally believe that the making of a complaint to the Data Protection Commissioner is the main remedy available to them for breaches of those rights and do not consider the possibility of commencing civil proceedings against the parties breaching their rights. The author of the present national report understands that no legal proceedings have actually been commenced in this context.

---

50 *Bunt* v. *Tilley et al*, *ibid*, par [22]. The passage is quoted in Cox & McCullough, *Defamation Law and Practice*, *op. cit*, p. 41, par. [2-46], Fn. 94. Mr. Justice Eady considered that internet operators can be judged according to the legal standards which have been applied to newspaper and other editors for over a century. He distinguished (i.e. considered to be irrelevant) the case of *Godfrey* v. *Demon Internet Ltd*, [2001] Law Reports, Queen's Bench 201, where the defendant became aware of a defamatory statement posted on its bulletin board only when asked by the claimant to remove that statement. These circumstances are now governed by Art. 18(1)(b) of the European Communities (Directive 2000/31/EC) Regulations 2003, which has been considered above, in the previous paragraph under the present point 2.2.1.3. of the present national report.

51 Refer to Milmo & Rogers [eds], *Gatley on Libel and Slander*, *op. cit*, p. 197, par. 6.31, especially at Fn. 241. That commentary considers the legal position in England and Wales. It is submitted that the position in Ireland is essentially the same.

52 Information provided to the author of this national report by Mr. Paul Durrant, Chief Executive of the Internet Service Providers Association of Ireland, during a discussion held on 05.06.2015.

53 *Report of the Internet Content Governance Advisory Group*, *op. cit*, p. 41, at Fn. 127.

54 Section 7 of the Data Protection Act 1998, amended by the Data Protection (Amendment) Act 2003. The electronic text is freely available on the website for Irish legislation (*electronic Irish Statute Book*), *op. cit*.

55 Refer to P. Lambert, *Data Protection Law in Ireland – Sources and Issues*, Dublin: Clarus Press, 2013, pp. 87 *et seq*, particularly at 107 – 108 and see also p. 126, under the heading, "Civil".

56 *Report of the Internet Content Governance Advisory Group*, *op. cit*, p. 41, at Fn. 128.

2.2.2. Soft law mechanism for removal

In overview, a **self-regulatory mechanism**, which could be described as "soft law", operates in Ireland with the aim of having internet content taken down if it breaches **Irish criminal law in a small number of specific fields**. This mechanism takes the form of a **hotline** coupled with an undertaking by Irish internet host providers to take down offending material which is found to be hosted in Ireland and a reciprocal cooperation agreement with "hotline" organisations in other countries.

The **practically most important**[57] **criminal offences** addressed by this mechanism are those included within the scope of what is generally referred to in Ireland as **"child sexual abuse"**. According to the website[58] of the Irish Internet Hotline, this includes child pornography, child trafficking, child sex tourism and the grooming of children for sex. The first two categories refer to the principal criminal offences set out[59] in the Child Trafficking and Pornography Act 1998, namely the offences of sexually exploiting a child, of trafficking, taking, detaining or restraining the personal liberty of a child for the purposes of sexual exploitation, of allowing a child to be used for child pornography and of producing, distributing, importing, exporting, selling, showing or possessing child pornography. The third category refers to the ancillary offences set out[60] in the Sexual Offences (Jurisdiction) Act 1996, which primarily permits the prosecution in Ireland of Irish citizens or permanent residents who commit certain sexual offences in foreign countries. The ancillary offences are those of transporting or arranging or authorising the transport of a person out of Ireland knowingly for the purpose of the commission of one or more of those sexual offences and of publishing information which promotes the commission of one or more of those sexual offences.[61] As no Irish criminal offence expressly refers to "grooming", the last category probably refers[62] to the offence, set out[63] in subsection 6(1) of

---

57 Over 4'800 reports were made to the Irish internet hotline in 2014. Of those, all but 100 concerned child sexual abuse. Refer to ISPAI Hotline.ie Service, *Annual Report 2014*, Dublin: 2015, unnumbered pages headed "Targeted services", "Illegal report analysis" and "Focus – illegal reports". The various figures, for reports in total and reports of individual criminal offences, do not add up, probably because some reports could be referred to more than one criminal offence or to no specific criminal offence.

58 http://www.hotline.ie/whatyoucanreport.php, directly after the heading, "Types of Illegal Content".

59 The original legislation was enacted as No. 22 of 1998. It was amended by section 6 of the Criminal Law (Sexual Offences) (Amendment) Act 2007, No. 6 of 2007, by sections 3 and 11 of the Criminal Law (Human Trafficking) Act 2008, No. 8 of 2008 and by section 3 of the Criminal Law (Human Trafficking) (Amendment) Act 2013, No. 24 of 2013. We are not aware of a consolidated version of the legislation as it currently stands, but links to all the amendments are available via the "Legislation Directory Entry" relating to the Child Trafficking and Pornography Act 1998 in the *electronic Irish Statute Book*), *op. cit*.

60 The legislation was enacted as No. 38 of 1996, is freely available in electronic form on the website for Irish legislation (*electronic Irish Statute Book*), *op. cit*. and has not been substantially amended in the meantime.

61 Refer to A.A. Gillespie, *Sexual Exploitation of Children – Law and Punishment*, Dublin: Round Hall / Thomson Reuters, 2008, pp. 26 to 30.

62 Proceeding on the basis of the contents of Chapter 5, "Grooming", in Gillespie, *Sexual Exploitation of Children – Law and Punishment, ibid*.

63 Section 6 of the Criminal Law (Sexual Offences) Act 1993, No. 20 of 1993, referring back to sections 1 and 2 of the Criminal Law Amendment Act 1935, No. 6 of 1935, originally criminalised soliciting for the purposes of homosexual acts with minors or of "defilement" of girls under the age of 17 and was coupled with the offence of soliciting for the purposes of prostitution. It was replaced, by section 2 of the Criminal Law (Sexual Offences) (Amendment) Act 2007, No. 6 of 2007, with a new text which expressly applies the offence regardless of whether or not prostitution is foreseen. Refer to Gillespie, *Sexual Exploitation of Children – Law and Punishment, ibid*, pp. 120 to 122.

the Criminal Law (Sexual Offences) Act 1993, of soliciting or importuning a child for the purpose of committing an act which would constitute one of a specified range of sexual offences, or to one of the mirror offences, of arranging to meet a child for the purpose of his or her sexual exploitation, which were subsequently introduced[64] into the Child Trafficking and Pornography Act 1998.

The Irish Internet Hotline also encourages[65] internet service providers and users to report instances of **online incitement to hatred and of racist or xenophobic content**. Under the Prohibition of Incitement to Hatred Act 1989, it is a criminal offence for any person to "publish … written material",[66] or to "distribute, show or play a recording of visual images or sounds",[67] which is or are "threatening, abusive or insulting and are intended or, having regard to all the circumstances, are likely to stir up hatred"[68]. It is similarly an offence to be involved in broadcasting "an item involving threatening, abusive or insulting visual images or sounds"[69] that are intended or likely to stir up hatred. The concept of "hatred" is tautologously explained as referring to

> "… hatred against a group of persons in the State or elsewhere on account of their race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation".[70]

Seen in the light of this legislative backdrop, the category of "racist or xenophobic content" is most probably one specific example of material which can be reported to the Irish Internet Hotline on the basis that it involves "incitement to hatred". The legislation, which was enacted before the internet age and has not been amended in the meantime, makes no reference to the online context. It is however, formulated in terms sufficiently broad to include online incitement to hatred.[71] Thus, the statutory concept of "publishing" is frequently encountered in common law jurisdictions like Ireland[72] and applies to the uploading of freely accessible internet content, at least in so far as it is actually accessed in Ireland.[73] The concept of broadcasting is defined in the Prohibition of Incitement to Hatred Act 1989 to mean:

---

64 Subsections 3(2A) and 3(2B) were inserted into the Child Trafficking and Pornography Act 1998 by section 6 of the Criminal Law (Sexual Offences) (Amendment) Act 2007, No. 6 of 2007. The former applies to a person who communicates with a child on at least two occasions and then travels with the intention of meeting the child, or actually meets the child, in Ireland for the purpose of his or her "sexual exploitation", a concept defined extensively in subsection 3(3) of the Child Trafficking and Pornography Act 1998, which was also inserted in its present terms by section 6 of the Criminal Law (Sexual Offences) (Amendment) Act 2007, No. 6 of 2007. The latter applies to an Irish citizen or permanent resident who behaves in this manner outside the country.

65 http://www.hotline.ie/whatyoucanreport.php, at the first "Note:".

66 Par 2(1)(a) of the Prohibition of Incitement to Hatred Act 1989, No. 19 of 1989.

67 Par 2(1)(c), *ibid*.

68 Final phrase of subsec. 2(1), *ibid*.

69 Subsec. 3(1), *ibid*.

70 Subsec. 1(1), *ibid*.

71 *Report of the Internet Content Governance Advisory Group*, *op. cit*, p. 41, before Fn. 125.

72 Perhaps most frequently in the context of the tort of defamation; compare above, the explanations given in the second-to-last paragraph under point 2.2.1. of this national contribution to the present study.

73 Refer to Gillespie, *Sexual Exploitation of Children – Law and Punishment, ibid*, p. 29 at par 2-70 and pp. 149 and 150 at pars. 6-104 to 6-109, citing the unreported judgment handed down on 19.07.2015 by Mr. Justice White of the High Court of Ireland in the case of *USA Rugby Football Union Limited* v. *Calhoun*.

> "… the transmission, relaying or distribution by wireless telegraphy or by any other means or by wireless telegraphy in conjunction with any other means of communications, of sounds, signs, visual images or signals, intended for direct reception by the general public …".[74]

Finally, the Irish Internet Hotline also encourages[75] internet service providers and users to report **"financial scams"**. It is not at all clear which criminal offences are referred to by this designation. In 2013, 64% and in 2014 45% of all reports allocated by the hotline to this category actually concerned "Trojan horse" malware pretending to originate from the Irish police and demanding electronic payment of a fine as a prerequisite to the "unlocking" of the recipient's computer.[76] The *Annual Report 2014* of the Irish Internet Hotline refers more generally to "phishing and other e-mail scams".[77] It therefore appears that the designation refers to all the criminal offences which can be committed by a person who attempts to defraud another of sums of money.

3. Procedural Aspects

What bodies are competent to decide to block, filter and take down Internet content? How is the implementation of such decisions organized? Are there possibilities for review?

3.1. Removal as a result of injunctive relief

The only **hard law mechanism for removal** or "take down" of unlawful internet content in Ireland is that of obtaining a judicial injunction ordering the content provider or internet host to remove the content.[78]

The **ordinary law of civil procedure[79] governs** claims for injunctive relief in respect of internet content. The applicant must arrange for the issuance and service on the defendant(s) of an initiating summons which commences standard civil proceedings in the only court with inherent, equitable jurisdiction to issue injunctions, namely the High Court of Ireland.[80] Final and permanent injunctions are normally settled and issued by the Court after the conclusion of a trial. In cases is which the removal sought by the applicant is practically complicated, or in which the judgment imposes practical limitations or conditions upon the injunctive relief to be granted, the judge may ask the parties' lawyers to work together to draft the detailed terms of the injunction and present it to him for approval.[81] A judgment granting injunctive relief is subject to the same **avenues of appeal** as any other judgment in civil proceedings for which no special appellate provision has been made.[82]

---

74 Subsec. 1(1) of the Prohibition of Incitement to Hatred Act 1989.

75 http://www.hotline.ie/whatyoucanreport.php, at the second "Note:".

76 ISPAI Hotline.ie Service, *Annual Report 2014*, *op. cit*, unnumbered page headed "Focus – Illegal Reports".

77 *Idem*.

78 Refer above, to point 2.2.1. of this national contribution to the present study.

79 Refer in particular to Order 50, Rule 12 of the Rules of the Superior Courts

80 By virtue of Orders 1 and 9 of the Rules of the Superior Courts. Refer also to the *Report of the Internet Content Governance Advisory Group*, *op. cit*, p. 46, at Fn. 148.

81 By virtue of Orders 41 and 115 of the Rules of the Superior Courts. Refer also to the second to last paragraph under point 2.2.1.1. above, where the preparation of an injunction following the delivery of the judgment in the case of *Sony Music Entertainment (Ireland) Limited et al.* v. *UPC Communications Ireland Limited* (No. 1), *op. cit*, is briefly described.

82 By virtue of Orders 58 (appeals to the Supreme Court) and 86A (appeals to the Court of Appeal) of the Rules of the Superior Courts. These rules permit appeals from "any judgement or order". The Rules of

As a matter of legal principle, **injunctive relief can be granted on an "interlocutory" basis (i.e. provisionally**, pending the resolution of the applicant's substantive claim at the end of the civil proceedings) and interlocutory injunctions can be granted after *ex parte* hearings (i.e. proceedings in which only the applicant's representatives make submissions to the judge, **before the intended respondent is notified of the application**) if the matter is particularly urgent and/or if irreparable damage is threatened.[83] The burden is upon the applicant in such cases to convince the judge that (i) his claim raises at least "a serious question to be tried", (ii) an award of damages would be an insufficient remedy of the harm sought to be prevented or limited by injunction and (iii) the "balance of convenience" favours the imposition of a restraint upon the (intended) respondent rather than patience on the part of the applicant pending the outcome of the proceedings.[84] The Irish courts have **accepted the view expressed by the European Court of Human Rights** that they should be reluctant to impose prior restraints upon free speech.[85] The leading commentary on Irish defamation law suggests[86] that this reluctance primarily influences the consideration by Irish judges of the "balance of convenience" in respect of applications to prevent or interrupt communications, in the sense that such applications are unlikely to succeed. The Supreme Court of Ireland has taken a clearer stance however, holding[87] that, when the applicant is seeking injunctive relief of a mandatory nature,[88] he must establish, under element (i) of the three-point-test described above, that his claim is so strong that it would be more likely than not to succeed at the full trial of the issues.

3.2. Mobile Alliance

The author of the present national report has been **unable to obtain any details of the procedure** through which the access of subscribers to certain internet content can be blocked by operators belonging to the Mobile Alliance Against Child Sexual Abuse Content.[89] We are therefore unable to indicate whether or when the decision to block is notified to the provider of the content blocked and whether that provider has any possibility of obtaining an independent review of the decision.

---

the Superior Courts do not specifically refer to injunctions, but include them within the concept of "orders"; refer to Order 41, Rule 8 and to H. Delany & D. McGrath, *Civil Procedure in the Superior Courts*, 3rd ed, Dublin: Round Hall / Thomson Reuters, 2012, p. 780, par. 24-21.

83 This power was conferred upon the High Court by subsec. 28(8) of the Supreme Court of Judicature (Ireland) Act 1877.

84 This test was initially formulated in the case of *Campus Oil* v. *Minister for Industry and Energy* (No. 2), [1983] Irish Reports 88.

85 Refer to Delany & McGrath, *Civil Procedure in the Superior Courts*, *op. cit*, pp. 428 to 431, citing the judgments of the European Court of Human Rights in *The Observer* & *The Guardian* v. *United Kingdom*, (1991) 14 European Human Rights Reports 153, in *Steel* and *Morris* v. *United Kingdom*, [2005] Entertainment and Media Law Reports 314; [2005] All England Reports (Digest) 207 (Feb) and in *Obukhova* v. *Russia*, unreported judgment of Section 1 of 08.01.2009 in respect of Applic. No. 34736/03 as well as the judgments of Mme. Justice Carroll of the High Court of Ireland in *Attorney General for England and Wales* v. *Brandon Book Publishers Ltd*, [1986] Irish Reports 597, and of Mr. Justice Clarke of the High Court of Ireland in the combined cases of *Cogley* v. *RTÉ*; *Aherne* v. *RTÉ*, [2005] 4 Irish Reports 79.

86 *Ibid*, pp. 431 *et seq*, pars. [12-12] *et seq*.

87 In the case of *Maha Lingham* v. *Health Service Executive*, [2006] 17 Employment Law Reports 137.

88 I.e. an injunction ordering the addressee to take action, rather than to simply refrain from or discontinue an action. An order to remove internet content would presumably be mandatory in nature.

89 Compare above, point 2.1.2. of the present national contribution to the present study.

3.3. Removal resulting from reports to Hotline.ie

Hotline.ie is an **operational unit** of,[90] or service provided by,[91] the Internet Service Providers Association of Ireland. The unit is **staffed by** content analysts who are employed by the ISPAI and work in premises which are located at ISPAI headquarters in Dublin, but physically separated from the ISPAI secretariat and separately secured. All content analysts have obtained university degrees in either law or information technology. They are specifically trained in-house by the ISPAI, together with the employees of hotlines in other countries by the International Association of Internet Hotlines (INHOPE) and by INTERPOL.[92]

Reports received by the unit are entered into the Hotline Operational Database. Analysts then try to obtain access to the reported internet content. If successful, the **analysts subsequently assess the legality of the content according to Irish law**.[93] That assessment is carried out in application of detailed guidelines and best practices which are based upon the Child Trafficking and Pornography Act 1998 and the Prohibition of Incitement to Hatred Act 1989 and are set out in a *Hotline Procedures Manual*.[94] If the assessment results in a finding that the internet content is not illegal according to Irish law prohibiting child sexual abuse material, racism and xenophobia or financial fraud,[95] then the reporter (assuming that she provided contact details, rather than reporting anonymously) is re-contacted and informed that the ISPAI will take no further action. If the assessment results in a finding that the internet content is illegal, then the Hotline's analysts make efforts to geo-locate the server on which it is loaded.[96] If that server is located in Ireland, a "takedown notice" is issued to the internet service provider who controls the server.[97] ISPs who are members of ISPAI are obliged by the ISPAI Code of Practice and Ethics to comply with such notices "within a reasonable time … [p]rovided it is technically practical to do so".[98] It is only at this point that the **party (content provider) affected by the decision to remove internet content receives a notification of that decision**. A specifically competent unit of the Irish police force is also notified of the finding.[99] The affected Member-ISP may be required to retain a copy of the content removed, as well as meta-data to assist any subsequent criminal investigation; it seems[100] that this is obligatory only when the police expressly request the retention of the information and that the obligation arises subject to the technical capacities of the ISP and the provisions of the Data Protection Act 1988. If the relevant server is found to be located outside of Ireland, but in a country which has a

---

90 This description was provided to the Institute by Mr. Paul Durrant, Chief Executive of the ISPAI and Manager of the hotline, by e-mail of 07.07.2015.

91 This is the description employed in ISPAI Hotline.ie Service, *Annual Report 2014*, *op. cit*.

92 This information was provided to the Institute by Mr. Paul Durrant, Chief Executive of the ISPAI and Manager of the hotline, by e-mail of 07.07.2015.

93 ISPAI Hotline.ie Service, *Annual Report 2014*, *op. cit*, unnumbered page headed "The Assessment Process".

94 This information was provided to the Institute by Mr. Paul Durrant, Chief Executive of the ISPAI and Manager of the hotline, by e-mail of 11.08.2015. Refer also *ibid*, to the unnumbered page headed "Annual Comparison", under the heading "Assessment Criteria" and to the hotline website: http://www.hotline.ie/processingreports.php (last consulted on 19.08.2015).

95 Compare above, point 2.2.2. of this national contribution to the present study.

96 ISPAI Hotline.ie Service, *Annual Report 2014*, *op. cit*, unnumbered page headed "The Assessment Process".

97 *Idem*.

98 Internet Service Providers Association of Ireland Ltd, *Code of Practice and Ethics*, Dublin, 2002, p. 13, par. 7.3.

99 ISPAI Hotline.ie Service, *Annual Report 2014*, *op. cit*, unnumbered page headed "The Assessment Process". Refer also to the unnumbered page headed "Working with Partners", under the subheading "An Garda Siochána".

100 According to the ISPAI *Code of Practice and Ethics*, *op. cit*, p. 13, par. 7.4.

hotline service belonging to INHOPE, then all available information is transferred to that service so that it can take the equivalent steps in that country. If the relevant server is found to be located outside of Ireland and in a country which does not have a hotline service belonging to INHOPE, then all available information is transferred to the law enforcement authorities of that country, via the competent unit of the Irish police force and INTERPOL.[101]

The *Hotline Procedures Manual* has not been published and its contents are treated as confidential.[102] This policy has been adopted by the hotline service on the basis that knowledge of its contents could assist criminals in avoiding detection and removal of illegal content and could facilitate hacker attacks against the hotline.[103] As a result, the interpretation of the law which underlies the hotline's analyses of internet content, as well as its procedures in dealing with content so analysed, are not directly subject to public scrutiny and comment. The ISPAI is at pains to point out that all of the Manual's contents, including recent modifications, have been "discussed and agreed"[104] with the Internet Safety Advisory Committee. This organism has been created, by the Office for Internet Safety belonging to the Department of Justice and Equality,[105] as the "stakeholder forum" required by the EU for funding of the Safer Internet Ireland Project and in order to advise the Office on internet safety in general, more especially the protection of children in relation to the internet and specifically the self-regulatory framework maintained by the ISPAI.[106] Its members include representatives of the public sector (police, Office for Internet Safety and Office of the Data Protection Commissioner), industry (including technology developers and the association of Irish mobile phone service providers ICIA) and civil society (including the National Parents Council and the Irish Society for the Prevention of Cruelty to Children).[107] This consultation mechanism, together with the Office for Internet Safety's "oversight" of the internet service industry,[108] permits indirect public scrutiny of the policy and practice applied by hotline.ie.

Being a private industry initiative, hotline.ie is **not subject to judicial review and its decisions** to require ISPs to remove internet content **cannot be appealed to a court or other public institution**. Detailed procedural provision has been made, on the other hand, for the **internal consideration of complaints**. Complaints are primarily expected to be made against members of the ISPAI, alleging that those members have not actually complied with one or more of their obligations under the ISPAI *Code of Practice and Ethics*.[109] The complaints procedure begins with the encouragement of informal

---

101 ISPAI Hotline.ie Service, *Annual Report 2014*, *op. cit*, unnumbered page headed "The Assessment Process".

102 This information was provided to the Institute by Mr. Paul Durrant, Chief Executive of the ISPAI and Manager of the hotline, by e-mail of 11.08.2015. Copies of the Manual, as updated from time to time, are provided only to the Irish Department of Justice, the Irish police force and the European Commission on the basis of assurances of confidentiality.

103 *Idem*.

104 *Idem*.

105 The website of the Office is to be found at http://www.internetsafety.ie/ It is listed on the website of the Department for Justice and Equality (http://www.justice.ie/en/JELR/Pages/AgenciesAndOffices) as an "Executive Office" of the Department. Both sites were last consulted on 24.08.2015.

106 Refer to the five points listed under the heading, "What will it have responsibility for?", on the internet page dedicated by the Office for Internet Safety to presentation of the Committee: http://www.internetsafety.ie/website/ois/oisweb.nsf/page/aboutus-ISAC-en (last consulted on 24.08.2015).

107 Refer *ibid*, to the persons listed under the heading, "Who are the members of the Internet Safety Advisory Committee?"

108 Refer in particular to http://www.internetsafety.ie/website/ois/oisweb.nsf/page/regulation-howitworks-en (last consulted on 24.08.2015), where the Office for Internet Safety threatens legislative intervention if self-regulation is ever considered not be functioning properly.

109 *Op. cit*, p. 17, par. 11.2.

resolution through contact with the ISP complained about, permits written responses to complaints for the ISPAI's secretariat when informal resolution efforts have proven unsuccessful and foresees a hearing before a Complaints Panel in the last instance.[110] If a Complaints Panel Report finds that an ISPAI member has breached its obligations, ISPAI's Board of Directors has the power to sanction that member.[111] A second avenue for complaints is specific to hotline.ie. The website of the service invites any "member of the public" with "a grievance" to submit a complaint specifying

> "… how the complainant believes the www.hotline.ie service has breached the INHOPE code of practice or the Hotline's own procedures in providing its service".[112]

This procedure involves an informal resolution mechanism, with the possibility of lodging a formal complaint for resolution by "the Hotline General Manager".[113] Finally, INHOPE offers a procedure for the resolution of complaints against national hotline operators belonging to that umbrella organisation. Complaints can therefore be lodged at the international level, against ISPAI, in respect of its operation of hotline.ie, or more specifically on the basis that ISPAI has allegedly breached the INHOPE *Code of Practice*.[114] This procedure is extremely similar to ISPAI's own complaints procedure,[115] culminating in a hearing before a complaints panel.[116] In response to an enquiry, ISPAI has confirmed[117] that these complaints procedures could be used to challenge a decision of the hotline.ie service to require the removal of certain internet content. ISPAI's Chief Executive assured[118] the author of the present national report that such complaints would be taken very seriously, as it is entirely conceivable that mistakes could be made, by the staff of the service or by the member ISP required to actually take down the relevant content: clerical or technical errors could result in the removal of the wrong content; an incorrect interpretation of the law could result in the removal of lawful content. According to the Chief Executive, no such complaint has ever been made, however. The very few complaints that have been formally lodged were all made by reporters dissatisfied by the fact that content which they had reported was not removed as a result.[119] Furthermore, all admissible complaints lodged during his period of office were resolved to the satisfaction of the complainants. The Complaints Panel has never actually been convoked.

4. General Monitoring of Internet

The author of the present national report has received **no information indicating that any entity in Ireland monitors internet content in general**. As part of the ongoing public debate on internet

---

110 *Op. cit*, pp. 17 and 18, pars. 11.7 to 11.8.5.

111 *Op. cit*, p. 19, pars. 12.1 and 12.2.

112 Second paragraph on http://www.hotline.ie/complaintsprocedure.php (last consulted on 24.08.2015).

113 Refer *ibid*, to the fifth and following paragraphs.

114 Association of Internet Hotline Providers, *Code of Practice*, Goring, United Kingdom, 2004, p. 4, defining the term, "Complaint".

115 The INHOPE *Code of Practice* was adopted two years after and largely copied from the ISPAI *Code of Practice and Ethics*.

116 Association of Internet Hotline Providers, *Code of Practice*, *op. cit*, pp. 13 to 16.

117 In an e-mail of 11.08.2015, sent to the Institute by Mr. Paul Durrant, Chief Executive of the ISPAI and Manager of the hotline.

118 *Idem*.

119 *Idem*. The ISPAI does not publish statistics of complaints received. The informal complaints of which Mr. Durrant is aware referred to internet content which the hotline.ie service had determined was not illegal, because it was hosted in the USA and protected by the first amendment to the US federal constitution. The complainants chose not to lodge formal complaints, but rather to make reports directly to the Irish police.

governance, the Internet Service Providers Association of Ireland consistently argues[120] that ISPs should not be asked to monitor the internet with the aim of identifying content which is unlawful or may be considered unacceptable

5. Assessment as to the case law of the European Court of Human Rights

5.1. Introduction

As far as we have been able to determine, Irish sources take **very little direct account of the case law of the European Court of Human Rights** of relevance to the blocking, filtering or removal of internet content.

This void largely results from the **structural or constitutional relationship of Ireland to the European Convention** for the Protection of Human Rights and Fundamental Freedoms. Following the common law tradition of England, the Republic of Ireland is a dualist jurisdiction in which rules of public international law have domestic effect only in so far as those rules are transposed into domestic law by the Irish legislature. In respect of the European Convention on Human Rights, the legislature enacted the European Convention on Human Rights Act 2003, which does not give direct effect to the Convention's provisions in Irish law; it only requires Irish courts to interpret Irish legislation and other "rules of law" in a manner compatible with Ireland's obligations under the Convention wherever possible[121] and permits the superior courts, "where no other legal remedy is adequate and available", to issue declarations that individual rules are incompatible with the Convention.[122] Such declarations have no impact upon the validity and application of the incompatible rules, however.[123] They simply warn the legislature of the incompatibility[124] and may result in the *ex gratia* payment of compensation to a party who suffers as a result of the incompatibility.[125]

Secondly, a number of human rights and fundamental freedoms are expressly or impliedly protected by the **Irish Constitution**. The Supreme Court of Ireland has recently held[126] that all claims invoking fundamental rights or freedoms must first be examined according to the relevant provisions of the Constitution and decided within the constitutional framework wherever possible. Only if the claims are unsuccessful within this framework, can an Irish court examine them in the framework of the European Convention on Human Rights and where appropriate, take the steps permitted by the European Convention on Human Rights Act 2003.

Thirdly, at least in the field of internet and communication law, the author of the present national contribution has the distinct impression that that the Irish commentators tend to give more attention to developments in the United States and the United Kingdom, than to the jurisprudence of

---

120 Refer for example to the ISPAI's press release of 26.07.2013 entitled, "Issue of Default Blocking of Pornographic Websites" and freely accessible on the ISPAI's website: http://www.ispai.ie/press-release-issue-of-default-blocking-of-pornographic-websites/#more-1327 (last consulted on 23.06.2015).

121 European Convention on Human Rights Act 2003, sec. 2.

122 European Convention on Human Rights Act 2003, subsec. 5(1).

123 European Convention on Human Rights Act 2003, par. 5(2)(a).

124 European Convention on Human Rights Act 2003, subsec. 5(3).

125 European Convention on Human Rights Act 2003, subsecs. 5(4) and (5).

126 In the case of *Carmody* v. *Minister for Justice and Equality*, [2010] 1 Irish Law Reports Monthly 157.

the European Court of Human Rights, , presumably as a result of cultural affinity.[127] On the contrary, they take full account of the **jurisprudence of the European Court of Justice** because, in the opinion of this author, European (Union) law is at least potentially directly applicable in Ireland.[128] Their analyses of that jurisprudence sometimes lead Irish commentators to consider European human rights law.[129]

The following summary of Irish appraisals of the compatibility of Irish regulation with European human rights law should be viewed in the light of these explanations.

5.2. ECHR principles and case law in Irish sources

5.2.1. Concerning online copyright infringements

Most of the discussion of human or individual rights affected by regulation of internet content in Ireland is to be found in, or at least concerns, the fight against copyright infringement on the internet.[130]

In the case[131] in which Norwich Pharmacal relief was first made available to Irish copyright holders complaining of infringements by internet users, Mr. Justice Kelly of the High Court of Ireland noted that the judicial jurisdiction under which such relief can be granted requires the plaintiffs' property rights to be weighed in the balance with the subscribers' competing rights of "confidentiality or privacy".[132] His Honour stated,[133] without citing any sources, that the subscribers' rights and the corresponding obligations of the internet service providers to preserve their privacy "may arise under statute, by contract or at common law". **Rights of confidentiality and privacy may not**, in the view of His Honour, **be relied upon by wrongdoers**, however. He concluded that the rights "must give way where there is *prima facie* evidence of wrongdoing"[134] and judicial relief is granted, not to prove the wrongdoing, but only to identify the alleged wrongdoers and thus effectively permit the plaintiff copyright holders to take civil action against them.

When considering a challenge mounted by the Data Protection Commissioner of Ireland against the legality of the agreement reached between Eircom and the major global sound recording enterprises,[135] Mr. Justice Charleton of the High Court expressly considered the Commissioner's **argument that the agreement breached the privacy rights of the subscribers who are warned and threatened with disconnection**. His Honour tersely recognised[136] that privacy is an "unenumerated

---

127 Refer for example to O'Dell, *Mechancial [sic.] turks, safe harbours, and immunities – liability for defamatory comments on websites*, *op. cit*, and to Hallissay, "Eircom, Injunctions and the European Union (Copyright and Related Rights) Regulations 2012", *op. cit*, at pp. 54-55.

128 In Lambert, *Data Protection Law in Ireland – Sources and Issues*, *op. cit*, for example, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is mentioned, on p. 28 at Fn. 49, only to the effect that it has been superseded by an EU Directive.

129 Refer below, to the last principal paragraph under point 5.2.1. of this national report, for an example.

130 Refer above, to point 2.2.1.1. of the current national report.

131 *EMI Records (Ireland) Limited et al*. v. *Eircom Limited* and *BT Communications Ireland Limited*, [2005] 4 Irish Reports 148.

132 *Ibid*, p. 152, par. 8.

133 *Idem*.

134 *Ibid*, p. 152, par. 10.

135 Refer above, to point 2.2.1.1. of the current national report.

136 *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, *op. cit,* par. 7.0 of the unreported judgment.

fundamental right" protected by Art. 40 of the Constitution of Ireland and that rights of privacy and communication are respectively guaranteed by Arts. 8 and 10 of the European Convention on Human Rights. He immediately went on[137] to characterise unauthorised exchanges of copyrighted works as having nothing to do with privacy. He considered[138] that a desire to ensure that wrongful activity remains undetected should not be confused with an exercise of privacy rights. Citing the judgment of the European Court of Justice in the case of *Scarlet Extended* v. *Société belge des auteurs, compositeurs et éditeurs SCRL*,[139] His Honour rejected the argument that the agreed "graduated response scheme" is equivalent to the implementation of telephone taps or house searches without judicial warrant, because there can be no legitimate expectation of privacy of communications made on peer-to-peer content exchange platforms.[140] After describing that case in some detail, His Honour quoted several passages from the ECJ's judgment in the similar case of *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA* v. *Netlog N.V.*[141] His Honour concluded[142] that the Data Protection Commissioner was wrong to rely upon those judgments, implying that they were based upon facts essentially distinguishable from the agreement entered into by Eircom. He considered[143] that a better guide is provided by a number of British decisions[144] in which the domestic courts of England and Wales granted injunctions against ISPs on the basis that that relief was specifically limited in scope, did not impose disproportionate costs upon the ISPs and represented an equitable "balance of burdens".

An Irish author has since **criticised[145] the initial determination of Justice Charleton that privacy rights are not engaged by arrangements to interrupt internet access** in reaction to criminal acts committed by the user by means of that access. The author pointed out[146] that His Honour went on to emphasise[147] that the "graduated response scheme" applied by Eircom involves no allegations that anyone has committed any crime. The author cited US and Canadian decisions holding that copyright infringements are inherently difficult to reconcile with the prerequisites to criminal liability[148] and that even where crimes (such as possession of child pornography) are committed by means of internet access, the perpetrator can rely upon his right to privacy, which the court would weight against competing rights of victims and interests of the community.[149] Finally, the author referred to

---

137 *Idem*.

138 *Ibid*, par. 7.1, first sentence.

139 Case C-70/10, [2009] European Court Reports I-1227.

140 *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, *op. cit,* par. 7.2 of the unreported judgment. His Honour quoted from the opinion of Advocate General Cruz Villalón and stated that the Court was right not to have adopted his proposals.

141 [2012] 2 Common Market Law Reports 18.

142 *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, *op. cit,* par. 8.10 of the unreported judgment.

143 *Idem*, pars. 8.8 and 8.9.

144 *Twentieth Century Fox Film Corporation et al.* v. *Newzbin Ltd*, [2011] Business Law Reports Digest 49; *Twentieth Century Fox Film Corporation et al.* v. *British Telecommunications plc*, [2012] 1 All England Reports 806; *Dramatico Entertainment Ltd* v. *British Sky Broadcasting Ltd et al*, [2012] 3 Common Market Law Reports 360.

145 O'Sullivan, "Irish Digital Rights in Retrograde: the 'Eircom Protocol' and the Normative Framework of European Law", *op. cit*, at pp. 366-367.

146 *Ibid*, at Fn. 45.

147 *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, *op. cit,* par. 10.1 of the unreported judgment.

148 *Dowling* v. *United States*, (1985) 473 United States Supreme Court Reports 207.

149 *R* v. *Cuttell*, (2009) 247 Canadian Criminal Cases (Third Series) 424, per Justice Pringle of the General Division of the Ontario Court of Justice. It is appropriate to note that upon the defendant's appeal, the Court of Appeal for Ontario held that his right to privacy had not been infringed (the appellate decision is reported at (2012) 296 Ontario Appeal Cases 324.

another English decision,[150] where it was held that an internet user's rights to private life and protection of personal data, guaranteed by Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union, are infringed whenever his identity is revealed to a third party without this permission. The author argued[151] that such an infringement can have a preponderant weight to the extent that a user may be wrongfully accused of wrongdoing, for example because his IP-address was misappropriated by another user (hacker) or because a third person, whom he permitted to use his internet access, breached the conditions of the permission.

Before concluding that he would grant an injunction in the case of *Sony Music Entertainment (Ireland) Limited et al.* v. *UPC Communications Ireland Limited* (No. 1),[152] Mr Justice Cregan cited a large number of sources, including Art. 1 of the Framework Directive for electronic communications networks and services.[153] He quoted[154] the full text of par. 3a, which requires measures taken by EU Member States to **respect the rights and freedoms guaranteed by the European Convention on Human Rights**. More specifically, it requires any measures to "be taken with due respect for the principle of the presumption of innocence and the right to privacy". Affected internet users are guaranteed "the right to be heard" as part of "[a] prior, fair and impartial procedure" which also includes "[t]he right to effective and timely judicial review …" Having considered relevant provisions of the Irish constitution and legislation and having reviewed relevant Irish and British jurisprudence, His Honour finally placed[155] most reliance upon the decisions of the European Court of Justice in the cases of *Scarlet Extended* v. *Société belge des auteurs, compositeurs et éditeurs SCRL*[156] and *UPC Telekabel Wien GmbH* v. *Constantine Film Verleih GmbH*,[157] particularly in **balancing the property rights of copyright holders with the freedom of internet service providers to conduct businesses under Art. 16 of the Charter of Fundamental Rights of the European Union**. It remains to be seen whether his judgment, in principle and in application to the specific terms of the injunction to be issued, will survive the scrutiny of the Court of Appeal of Ireland. It is however, probably pertinent to point out that the Supreme Court of Ireland, in deciding an earlier appeal[158] of essentially procedural issues and just before stating that it did not need to consider the substantive issues being discussed here, quoted[159] at some length from the judgment of Mr. Justice Charleton in *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, including the following passage:

> "… the nature of the injunction sought; the limitation to and the duration of any monitoring; the breadth or narrowness of the scope of any order; the nature of the equipment to be used; the potential for the interference of that equipment with the proper use of the existing

---

150 *Golden Eye (International) Ltd* v. *Telefonica UK Ltd*, [2012] All England Reports (Digest) 79 (Jul), per Justice Arnold of the Chancery Division of the High Court of Justice of England and Wales. His decision was contested in the Court of Appeal of England and Wales, but its judgment, reported at [2013] Business Law Reports 414; [2013] Entertainment and Media Law Reports 1, was limited to the standing of certain claimants to seek relief and did not concern the question of availability of remedies in general.

151 O'Sullivan, "Irish Digital Rights in Retrograde: the 'Eircom Protocol' and the Normative Framework of European Law", *op. cit*, p. 367, after Fn. 53.

152 *Op. cit*. Refer above, to the second to last paragraph under point 2.2.1.1. of the current national report.

153 Directive 2002/21/EC.

154 *Sony Music Entertainment (Ireland) Limited et al.* v. *UPC Communications Ireland Limited* (No. 1), *op. cit*, par. 111 of the unreported judgment.

155 *Idem*, at pars. 142 to 148.

156 *Op. cit*.

157 Case C-314/12, [2014] Business Law Reports 541.

158 *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner and Eircom Ltd (notice party)*, [2014] Irish Law Reports Monthly 225.

159 *Ibid*, at pp. 233-234.

> systems of the intermediary; the balance of the burden between the parties as to equipment, personnel and cost; the intrusiveness of any remedy into legitimate privacy and the entitlement to communicate; and any potential data protection impingements, together constitute the main factors in a court determining where the proportionality of an injunctive remedy to the mischief of the improper use of intellectual property online is to be struck or whether, on the other hand, an injunction application is to be refused, despite legal compliance, on discretionary grounds".[160]

5.2.2. Concerning defamation using internet platforms

Outside of the context of copyright infringement, human rights aspects are most frequently discussed in respect of defamation over the internet.

The Internet Content Governance Advisory Group was established by the Minister for Communications, Energy and Natural Resources to analyse Irish legislation governing, regulatory frameworks concerning and policy responses to issues arising out of internet content.[161] In its report of May 2014, the Group stressed[162] that the Irish constitution provides a framework for the protection of personal rights and freedoms which predates the European Convention on Human Rights and has a status within Ireland of pre-eminence over the Convention. Particular attention was drawn[163] to Article 40 of the Constitution. It guarantees "the right of the citizens to express freely their convictions and opinions",[164] but that guarantee is made "subject to public order and morality"[165]. It also recognises both the right to a "good name" and the "property rights of every citizen".[166] In this latter respect, the Constitution[167] obliges the State to "protect" the rights "by its laws … as best it may from unjust attack and, in the case of injustice done, vindicate …" the rights. The authors of the report stated that the law of **defamation "strives to find a constitutionally acceptable balance" between the freedom of expression and the right to protection of one's reputation ("good name")**.[168] The authors further explained that their work in the preparation of the report "… include[d] consideration of the governance, operation and vindication of those constitutional rights" "and by extension the European Convention rights (Articles 8 and 10)".[169]

A **detailed analysis of the relevant Convention provisions (Arts. 6, 8 and 10) and of relevant decisions of the European Court of Human Rights** is to be found in the leading Irish commentary on the law of defamation.[170] *Inter alia*, the authors criticise[171] the decision of the First Section of the Court in the case of *Delfi AS* v. *Estonia*[172], especially because it apparently failed to take account of

---

160 *EMI Records (Ireland) Limited et al.* v. *Data Protection Commissioner*, *op. cit,* par. 8.10 of the unreported judgment.

161 See the "Foreword by the Chairperson" to the *Report of the Internet Content Governance Advisory Group*, *op. cit*, p. 2.

162 *Ibid*, pp. 13 and 14.

163 *Ibid*, p. 13, under the heading, "Areas of focus".

164 Par. 6 point 1° i. of Art. 40 of the Irish Constitution.

165 Par. 6 point 1° of Art. 40 of the Irish Constitution.

166 Par. 3 point 2° of Art. 40 of the Irish Constitution.

167 Par. 3 points 1° and 2° of Art. 40 of the Irish Constitution.

168 *Report of the Internet Content Governance Advisory Group*, *op. cit*, p. 14, first and second paragraphs.

169 *Ibid*, fifth paragraph.

170 Cox & McCullough, *Defamation Law and Practice*, *op. cit*, pp. 467 to 513.

171 *Ibid*, pp. 511 and 512, pars. [13-105] and [13-106].

172 Unreported judgment of 10.10.2013 in respect of Applic. No. 64569/09. The text of the judgment is freely available in electronic form on the official internet site of the Council of Europe: http://hudoc.echr.coe.int/eng?i=001-126635 (last consulted on 25.08.2015).

the applicant's arguments that (i) the imposition of liability endangered the viability of the internet service, due to the cost of vetting users' comments before they are posted, that (ii) the need for such vetting would have a chilling effect on free speech, because the moderators would surely err on the side of caution and exclude any comments that might imaginably be considered defamatory by anyone and that (iii) the considerable public interest in the subject being commented upon might outweigh the need to protect individual reputations. In line with the common law tradition, the authors then try to confine the authority of the decision to the particular facts of the case, emphasising that the subject was of a nature that is likely to attract defamatory comments, that some of the comments were in fact threatening as well as defamatory and that the Court was very impressed by the potential of technology which it had not previously dealt with.

5.2.3. Concerning blockage and removal of internet content using soft law mechanisms

It would be useful, for the purposes of the present study, to determine whether and if so, the manner in which, account is taken of the need to protect freedom of expression in the internet when soft law mechanisms are applied in Ireland to block or remove specific internet content.

The available information does not allow us to make that determination. GSMA Europe, within the framework of which several Irish mobile telecommunications operators belonging to the Mobile Alliance Against Child Sexual Abuse Content block access to certain internet sites,[173] provides no information about the manner in which those sites are identified and designated. The Internet Service Providers Association of Ireland, operator of the Irish Internet Hotline, refuses to provide details of the decision-making procedures which lead to the designation of certain internet content as unlawful.[174] Its manual of procedures has however, been vetted by the Internet Safety Advisory Committee, an organism which permits indirect public scrutiny of the policies and practices applied in the operation of the removal mechanism.[175] It may be that account of the need to protect the freedom of expression has been taken by this organism and that this is reflected in the terms of the manual of procedures.

5.3. Evaluation

In respect of copyright protection in the context of the internet, Irish law expressly refers to the rights enshrined and the standards set in the European Convention on Human Rights and the jurisprudence of the European Court of Human Rights, albeit mostly indirectly, through the lens of European Union law.[176] In order to know whether Irish law also conforms to those rights and standards, it will be necessary to await the outcome of the appeal which is pending in the case of *Sony Music Entertainment (Ireland) Limited et al.* v. *UPC Communications Ireland Limited* (No. 1)[177] and discover the terms of any injunction which is actually issued at the conclusion of the proceedings.

In respect of defamation in the context of the internet, the existing case law does not expressly refer to the European Convention on Human Rights and the jurisprudence of the European Court of Human Rights, but it clearly does undertake to weigh competing rights and interests essentially similar to those protected by the Convention.[178] Given that the European Court of Human Rights in

---

173 Refer above, to points 2.1.2. and 3.2. of the current national contribution to the present study.

174 Refer above, to the third paragraph under point 3.3. of the current national contribution to the present study.

175 *Idem*.

176 Refer above, to points 2.2.1.1. and 5.2.1. of the current national contribution to the present study.

177 *Op. cit*. Refer specifically to the second to last paragraph under point 2.2.1.1. *ibid*.

178 Refer above, to points 2.2.1.2. and 5.2.2. *ibid*.

its own jurisprudence leaves each Member State a considerable margin of appreciation, Irish law as it currently stands in this respect is unlikely to be in breach of the Convention.

We are not aware of any sources of Irish law referring expressly to the need to preserve the right of freedom of expression when blocking access to or removing internet content. Publications discussing the freedom of expression in the context of removal of defamatory internet content have been presented above.[179] That the right of freedom of expression should be interfered with only on the basis of legal provisions, which balance competing rights and duties and limit the interference to that which is necessary in a free and democratic society, is a stance frequently taken by the Internet Service Providers Association of Ireland in response to calls for the industry to proactively filter out "harmful" internet content.[180] Beyond that, a pressing need to protect freedom of expression, on the internet and elsewhere, is not felt in Ireland. On the contrary, having visited Ireland and surveyed the Irish press, the author of the current national contribution to the present study is impressed by the pressure which interest groups, journalists and political actors frequently bring to bear on the Irish government to take steps aimed at reducing the "misuse of the internet" by criminals and generally "harmful" activity on the internet.

Martin Sychold
17.12.2015

Revised on 03.06.2016 taking into consideration comments from Ireland on this report

179 Under point 5.2.2. of the current national contribution to the present study.

180 Refer above, to point 4. of the current national contribution to the present study.